RSA SecurID Ready Implementation Guide

Last Modified: December 23, 2004

1. Partner Information

Partner Name	Citrix Systems, Inc.
Web Site	www.citrix.com
Product Name	Web Interface for MetaFrame Presentation Server
Version & Platform	3.0, Windows
Product Description	Citrix MetaFrame Presentation Server is the easiest way to manage enterprise applications from a central location and access them from anywhere. The foundation of the MetaFrame Access Suite, Citrix MetaFrame Presentation Server is the world's most widely deployed presentation server for centrally managing heterogeneous applications and delivering their functionality as a service to workers, wherever they may be. The Web Interface for MetaFrame Presentation Server extends this access to standard web browsers, increasing user mobility and flexibility.
Product Category	Remote Access

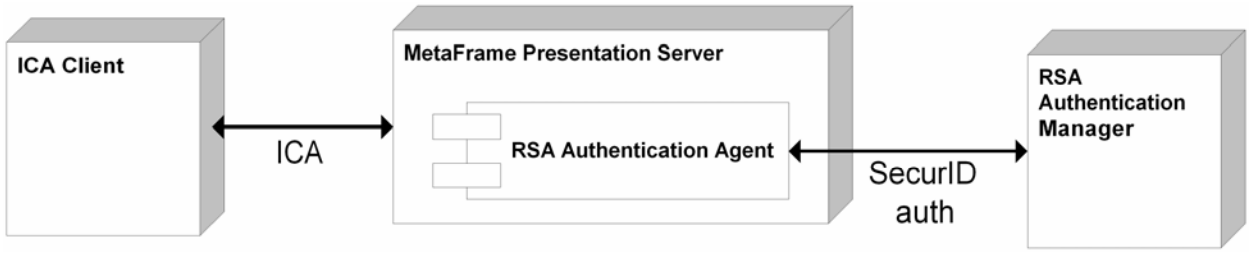
2. Contact Information

	Sales Contact	**Support Contact**
Phone	800-4CITRIX (US) 954-267-3000 (International)	800-4CITRIX (US) 954-267-3000 (International)
Web	www.citrix.com	www.citrix.com

3. Solution Summary

Citrix MetaFrame Presentation Server provides access to enterprise applications to local, remote, and mobile users over a variety of transports. One of these transports is HTTP. Users can utilize a standard web browser to access published resources via the Web Interface for MetaFrame Presentation Server. When exposing enterprise data, companies are concerned about positively identifying users attempting to access that data. Using strong two-factor authentication, RSA Authentication Manager creates an end-to-end trusted and secured solution for an enterprise.

Feature	Details
Authentication Methods Supported	Native RSA SecurID Authentication
RSA Authentication Agent Library Version	5.0.3
RSA Authentication Manager Name Locking	Yes
RSA Authentication Manager Replica Support	Full Replica Support
Secondary RADIUS Server Support	N/A
Location of Node Secret on Client	In Registry
RSA Authentication Agent Host Type	Net OS
RSA SecurID User Specification	All Users
RSA SecurID Protection of Partner Product Administrators	No
RSA Software Token API Integration	No



4. Product Requirements

Hardware requirements

Component Name: MetaFrame Presentation Server	
HD space	400-500MB, depending on install options

Software requirements

Component Name: MetaFrame Presentation Server *	
Operating System	**Version (Patch-level)**
Windows 2000	Server, Adv Server, Datacenter Server
Windows 2003	Server, Enterprise Server, Datacenter Server
JRE	1.4.1_02 or later

Component Name: MetaFrame Presentation Server Web Interface	
Operating System	**Version (Patch-level)**
Windows 2000	SP4, IIS 5.0
Windows Server 2003	IIS 6.0
JRE	1.4.1_02 or later
.NET Framework +	1.1
Visual J# .NET +	1.1
ASP.NET +	

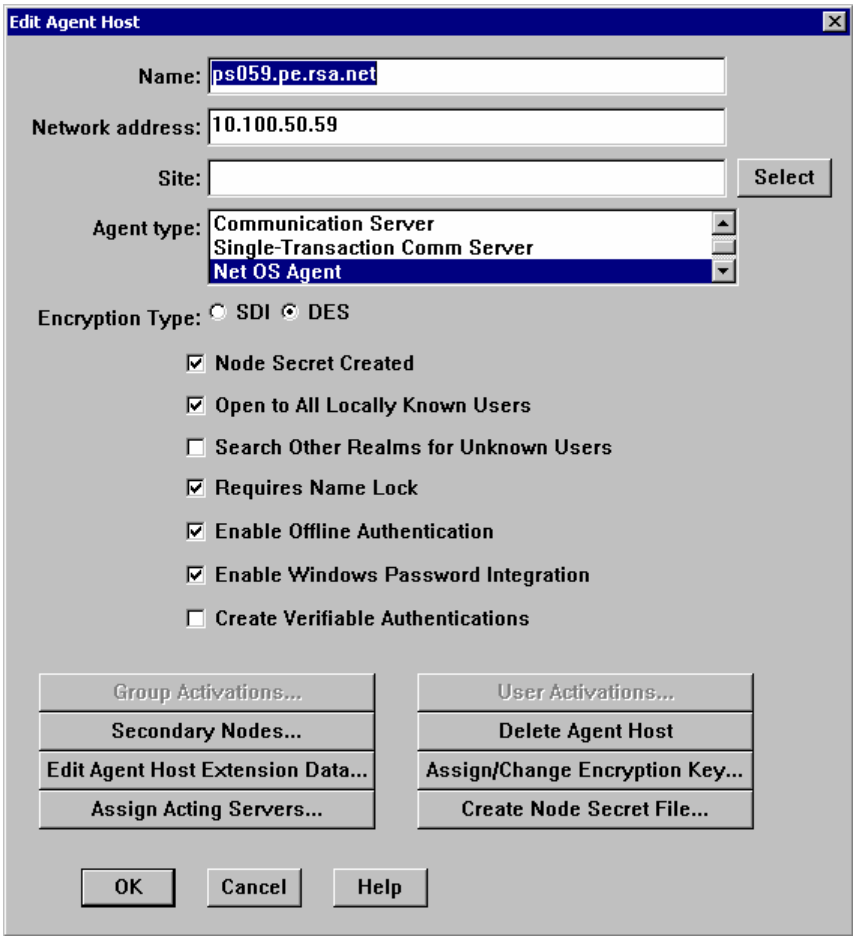
* Current requirements for specific patches are listed in the **MetaFrame Presentation Server 3.0 for Windows Pre-Installation Checklist**. The most current version of this, as well as any update bulletin, is available on the Citrix web site.

+ The redistributable files for these frameworks are included on the *MetaFrame Presentation Server* CD-ROM, in the support folder.

5. RSA Authentication Manager Configuration

If your Web Interface server is not already registered as an agent host, add it to the RSA Authentication Manager database as follows:

- Go to **Start > Programs > RSA ACE Server**, and then **Database Administration - Host Mode**.
- Then, from the **Agent Host** menu, choose **Add Agent Host…**.



- In **Name**, type the hostname of the MPS Web Interface.
- In **Network address**, type the IP address of the MPS Web Interface, if it is not automatically filled in as you leave the **Name** field.
- For **Agent Type**, select “Net OS Agent”.
- Under **Secondary Nodes**, define all other hostname/IP addresses that resolve to the MPS Web Interface, if needed.

Note: It’s important that all hostname and IP addresses resolve to each other. Please reference the RSA Authentication Manager documentation for detailed information on this and other configuration parameters within this screen. You can also select the ‘Help’ button at the bottom of the dialog.

6. Partner RSA Authentication Agent configuration

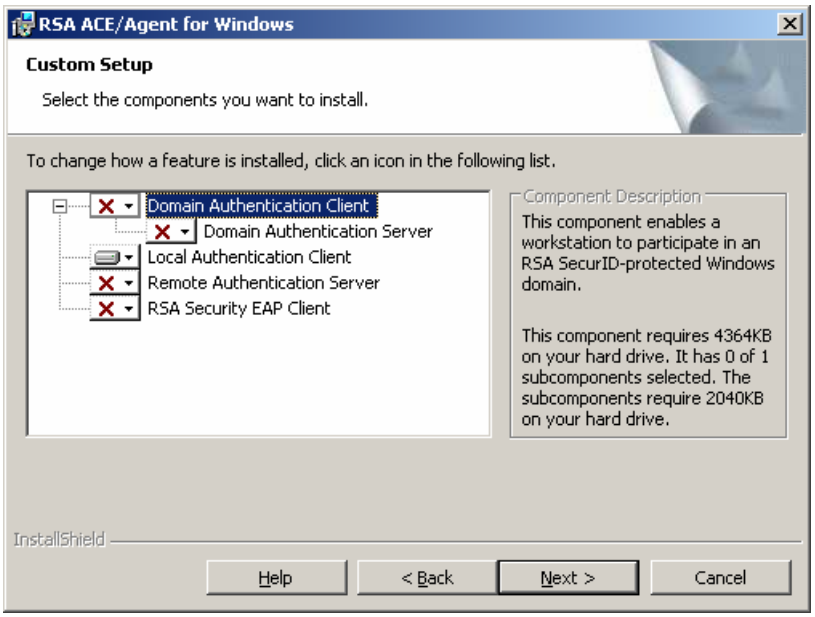
This section provides instructions for integrating the partners' product with RSA SecurID authentication. This document is not intended to suggest optimum installations or configurations. It is assumed that the reader has both working knowledge of the two products to perform the tasks outlined in this section and access to the documentation for both in order to install the required software components. All products/components need to be installed and working prior to this integration. Perform the necessary tests to confirm that this is true before proceeding.

For this integration, the products involved would be:

- ➔ RSA Authentication Manager
- ➔ RSA Authentication Agent for Windows
- ➔ Citrix MetaFrame Presentation Server
- ➔ Citrix MetaFrame Presentation Server Web Interface

RSA Authentication Agent Installation

For the purposes of this integration, the RSA Authentication Agent for Windows was installed as a local authentication client (LAC). This option must be explicitly selected during installation, since it is not the default.



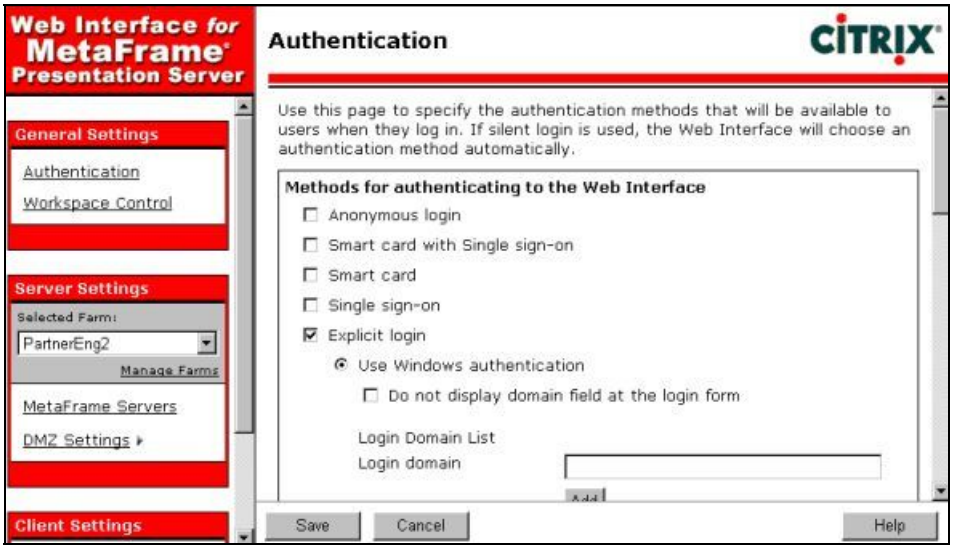
Note: Installation of the Authentication Agent is only required to ensure that the appropriate DLLs for SecurID authentication are available to the Web Interface SecurID module. Even though the agent used in this integration was v6.0, any agent v5.0 or later should work.

Enabling SecurID Authentication for the MPS Web Interface

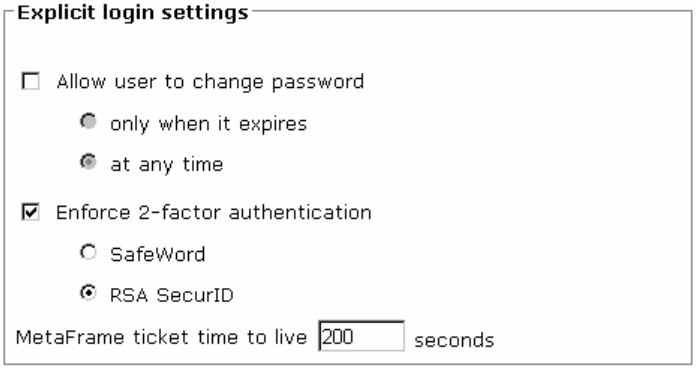
Prior to enabling RSA SecurID authentication, verify the permissions on the node secret. Launch regedt32, navigate to HKLM\SOFTWARE\SDTI\ACECLIENT, right-click on it, and select **Permissions**. In order for the Web Interface to be able to write the node secret into the registry, the following local machine accounts must have full access to this key; ASPNET, IUSR_*machinename*, and IWAM-_*machinename*. For more information on this, see Known Issue # 1.

Warning: Manually modifying registry settings may lead to errors that can render your system unusable. Please do not attempt to edit the registry unless you are comfortable with such activity, and willing to reinstall the operating system, should it become necessary

To enable SecurID authentication for users logging into the Web Interface, use the Web Interface Admin Tool. After starting the tool, click the **Authentication** link in the menu bar on the left side of the page.



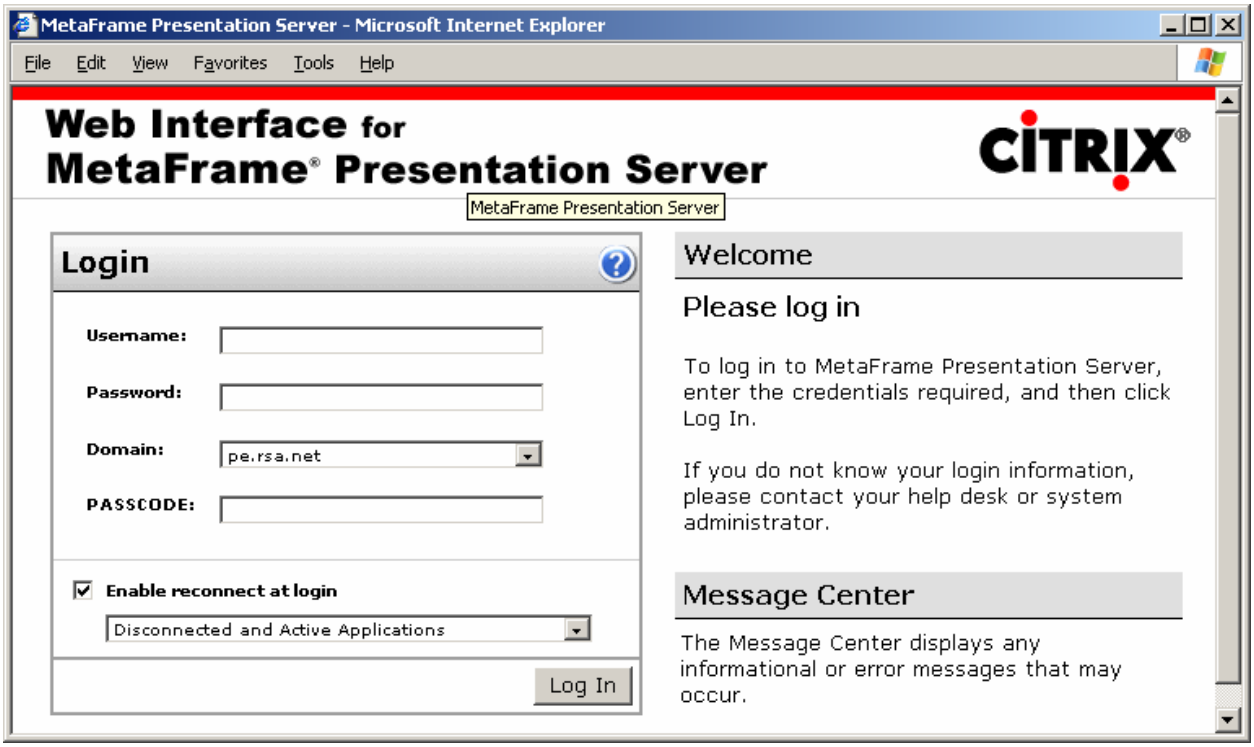
Ensure that the **Explicit login** box is checked to force users to supply a username and password to Web Interface. In the settings box at the bottom of the page, check the **Enforce 2-factor authentication**, and select **RSA SecurID**.



Save your changes, and then click the **Apply Changes** button.

Logging into Web Interface

Once these changes have been applied, you will be able to log into Web Interface using RSA SecurID authentication. All Web Interface users will be challenged, and this is not configurable. When using RSA SecurID authentication, users will be prompted for their PASSCODE, in addition to their username and password.



For additional information on the configuration of the MPS Web Interface with RSA SecurID authentication, see the *Web Interface Administrator's Guide*.

7. Certification Checklist

Date Tested: December 23, 2004

Tested Certification Environment		
Product	**Platform (OS)**	**Product Version**
RSA Authentication Manager	Windows 2003 Ent, IIS 6.0	6.0
RSA SecurID for Microsoft Windows	Windows 2003 Ent, IIS 6.0	6.0
RSA Software Token	Windows 2003 Ent, IIS6.0	3.0.3
Citrix MPS Web Interface	Windows 2003 Ent, IIS6.0	3.0

Test	RSA Native Protocol	RADIUS Protocol
1st time auth. (node secret creation)	P	
New PIN mode:		
User forced to authenticate after NewPin set	P	N/A
System-generated		
Non-PINPAD token	P	N/A
PINPAD token	P	N/A
User-defined (4-8 alphanumeric)		
Non-PINPAD token	P	N/A
Password	P	N/A
User-defined (5-7 numeric)		
Non-PINPAD token	P	N/A
PINPAD token	P	N/A
Software token	P	N/A
Deny invalid PIN length	F*	N/A
Deny Alphanumeric	F*	N/A
User-selectable		
Non-PINPAD token	P	N/A
PINPAD token	P	N/A
PASSCODE		
16 Digit PASSCODE	P	N/A
4 Digit Password	P	N/A
"Pin-less" TokenCode	P	N/A
Next Tokencode mode		
Non-PINPAD token	P	N/A
PINPAD token	P	N/A
Software Token API Authentication		
New PIN mode	N/A	N/A
8 Digit PIN with 8 Digit TokenCode	N/A	N/A
Failover	P	N/A
User Lock Test (RSA Name Lock Function)	P	
No RSA Authentication Manager	P	N/A

ATB

Pass, Fail or N/A (N/A=Non-available function)

* See Known Issue # 2 for details

8. Known Issues

1. Node Secret Permissions

If the Web Interface does not have permission to write the node secret into the registry, authentication will succeed once, then fail with a “Node verification failure”. If the node secret is cleared from the Authentication Manager console, authentication will again succeed one time. This happens due to the fact that the RSA Authentication Manager sends the node secret to an agent host following the first successful authentication from that host. From that point on, the RSA Authentication Manager requires all traffic from that host to be protected using the supplied node secret.

Previously, simply installing the RSA Authentication Agent prior to installing the Web Interface was enough to guarantee that the permissions for node secret were modified correctly. Under Windows 2003 and IIS 6.0, this does not appear to be the case. Currently, the local machines ASP.NET account (ASPNET), Internet Guest account (IUSR_*machinename*), and the Launch IIS Process Account (IWAM_*machinename*) are required to have full access to the node secret key. Information concerning this issue is also available from the Citrix support site, in document CTX102226, titled “Error: The credentials supplied were invalid. Please try again”

2. Invalid PIN not rejected

During certification testing, it was noticed that the Web Interface was not properly validating user entered PINs. When system settings on the RSA Authentication Manager were modified to restrict PINs to between 5 and 7 digits, the Web Interface accepted PINs of length 4 and 8. These PINs are rejected by the RSA Authentication Manager, but no error is returned to the user, leaving them in a confusing state. Also, when alphanumeric PINs are disabled, the same behavior is exhibited.

The easiest work-around for this issue is to use system-generated PINs.